FIP PUB 74
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 1981

GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, Secretary
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89.306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance and coordination of Government efforts in the development of guidelines and standards in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, DC 20234.

James H. Burrows, Director Institute for Computer Sciences and Technology

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 01-04-1995	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-1995 to xx-xx-1995

4. TITLE AND SUBTITLE Guidelines for Implementing and Using the NBS Data Encryption Standard Unclassified	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Baldridge, Malcolm ; Ambler, Ernest ;	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. Department of Commerce xxxxx xxxxx, xxxxxxx	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS FIPS ,	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
CATALOGERS: Date of Document and Dates Covered should be 1981

14. ABSTRACT
See report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
			Public Release	30	email from Booz Allen (IATAC), (blank) lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/1/1981	Report 4/1/1981

4. TITLE AND SUBTITLE
Guidelines for Implementing and Using the NBS Data Encryption Standard

5. FUNDING NUMBERS

6. AUTHOR(S)
Baldridge, Malcolm; Ambler, Ernest

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Department of Commerce

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
FIPS

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Data Encryption Standard (DES) w published u Federal Information Processing Standards Publication (WHOA PUB 46 on
January 15, 1977 [2]. The DES specifies a cryptographic algorithm for protecting computer data. WHOA PUB 81 [3] de~n~ four modes of operation for the DES which may be employed in a wide variety of applications. These guidelines are to ~ applied in conjunction with WHOA PUB 46 and WHOA PUB 81 when implementing and using the Data Encryption Standard They provide information on what encryption is, general guidance on how encryption protects against certain vulnerabilities of computer networks, and specific guidance on the DES mode of operation in data communications applications. When u~'d with the proper administrative procedures and when implemented in accordance with these guidelines, electronic device performing the encryption and decryption operations of the standard can provide a high

14. SUBJECT TERMS
IATAC Collection, computer security, cryptography, data integrity, encryption, Federal Information Processing Standards Publication, network security, security

15. NUMBER OF PAGES
29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Abstract

The Data Encryption Standard (DES) w published u Federal Information Processing Standards Publication (WHOA PUB 46 on January 15, 1977 [2]. The DES specifies a cryptographic algorithm for protecting computer data. WHOA PUB 81 [3] de~n~ four modes of operation for the DES which may be employed in a wide variety of applications. These guidelines are to ~ applied in conjunction with WHOA PUB 46 and WHOA PUB 81 when implementing and using the Data Encryption Standard They provide information on what encryption is, general guidance on how encryption protects against certain vulnerabilities of computer networks, and specific guidance on the DES mode of operation in data communications applications. When u~'d with the proper administrative procedures and when implemented in accordance with these guidelines, electronic device performing the encryption and decryption operations of the standard can provide a high level of cryptographic protect on '.o data in computer system and networks.

Key words: Computer security; cryptography; data integrity; encryption; Federal Information Processing Standards Publication; key distribution; network security; security.

Nat. Bur. Stand. (U.S.), Fed. Info. Prooers. Stand. Publ. (flPS PUB) 74, 39 pages.(1981)DEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161

PUB 74

1981 April 1

ANNOUNCING ThE

GUIDELINES FOR IMPLEMENTING AND USING ThE

NBS DATA ENCRYPTION STANDARD

Fed.ral 1nforrn£tion Processing Standaids Publications are 's.ued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline: Guidelines for Implementing and Using the NBS Data Encryption Standard (DES).

Category of Guideline: ADP Operations, Computer Security.

Explanation: The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its ADP systems. This publication provides guidelines to be used by Federal organizations when these organizations specify that cryptographic protection is required for sensitive or valuable computer data, Protection of computer data during transmission between electronic components or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by that data, These guidelines are to be applied in conjunction with FIPS PUB 46 and FIPS PUB 81 when implementing and using the Data Encryption Standard.

Approving Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Applicability: These guidelines are applicable whenever the DES is used for the cryptographic protection of computer data,

Implementation: These guidelines should be referenced in the formulation of plans by Federal agencies for the encryption of compute data using the DES.

Specifications: Federal Information Processing Standard 74 (FIPS PUB 74), Guidelines for Implementing and Using the NBS Data Encryption Standard (affixed).

Cross Index:

a, FIPS PUB 31, Guidelines to ADP Physical Security and Risk Management.
b. FIPS PUB 39, Glossary for Computer Systems Security.
c. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.
d. FIPS PUB 46, Data Encryption Standard.
e. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.
f. FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis.
g. FIPS PUB 81, DES Modes of Operation Standard.

Qualifications: These guidelines provide information which aids in the secure implementation of the DES. In addition it presents the considerations that are necessary when implementing cryptography and key management schemes. Some of the implementations described are not required methods but are for the reader's own information. However, the modes of operation are

specified by the DES Modes of Operation Standard (FIPS PUB 81 Cross Index g).

Export Control: Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, code of Federal Regulations, Parts 121 through 128. Cryptographic devices implementing these guidelines and technical data regarding them must comply with these Federal regulations.

Patents: Cryptographic equipment implementing these guidelines may be covered by U.S. and foreign patents.

Where to Obtain Copies of the Guideline: Copies of this publication are for sale by the National Technical Information Service, U.S.

Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 74 (FIPS-PUB-74) and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information Processing Standards Publication 74
1981 April 1
Specifications for

GUIDELINES FOR IMPLEMENTING AND
USING THE NBS DATA ENCRYPTION STANDARD

CONTENTS

Page

peg.

1. INTRODUCTION

Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, and requires protection. It is common to find data transmissions which constitute monetary transfers of billions of dollars daily. Sensitive information concerning individuals, organizations, and corporate entities is collected by Federal agencies in accordance with statutory requirements and is processed in computer systems. This information requires some type of protection, and cryptographic protection may be specified by the authority responsible for the data. The NBS Data Encryption Standard [2]* must be employed when cryptographic protection is required for unclassified Federal ADP data- The DES Modes of Operation Standard [3] defines the methods or modes in which the DES may be implemented.

The rapid growth of computer data banks increases the potential threats to personal privacy. Since data banks often are accessible from remote computer terminals, there is a threat of easy and unauthorized access to personal information from any place in the data communications system. Such information has typically been scattered in remote locations, controlled under separate auspices, and physically or administratively protected. With a telecommunications network of computer systems, what was previously a laborious job of assembling comprehensive dossiers on individuals may become a simple task◦ Thus, both valuable and sensitive information require protection against unauthorized disclosure and modification.

Encryption is a tool which may be used in data security applications. It is not a panacea. With improper implementation and use, data encryption may only provide an illusion of security. With inadequate understanding of encryption applications, data encryption could deter the utilization of other needed protection techniques. However, with proper management controls, adequate implementation specifications, and applicable usage guidelines, data encryption will not only aid in protecting data communications but can provide protection for a myriad of specific data processing applications.

2. DATA ENCRYPTION

2.1 What Is Data Encryption?

Data encryption is a process used to hide the true meaning of data. The word "encryption' has been coined from the word "cryptography" which was derived from the ancient Greek words "kryptos" (hidden) and "graphia" (writing). Encryption is the process of transforming text or data into an unintelligible form called cipher. Reversing the process of encryption and transforming the cipher back into its original form is called decryption. Encryption and decryption comprise the science of cryptography as it is applied to the modern computer.

2.2 How Is Data Encryption Achieved?

Data encryption is achieved through the use of an algorithm that transforms data from its intelligible form to cipher. An algorithm is a set of rules or steps for performing a desired operation. An algorithm can be performed by anything that can be taught or programmed to perform a specific and unambiguous set of instructions. Electronic devices which efficiently perform the mathematical steps of the algorithm spa-led in the Data Encryption Standard (DES) are described in theme guidelines.

2.3 Where Should Data Encryption Be Used?

Cryptography (encryption) has historically been used to protect sensitive information darn~ communication. It can be used for protecting computer data transmitted between terminals and computers or between computers. Data is encrypted before transmission and decrypted after it is received. The algorithm used to decrypt the received cipher must be the inverse of the algorithrm

'Numbers in brackets indicate references given in section 9.

used to encrypt the transmitted data. In general, a device used to transmit and receive data would contain algorithms for both encryption and decryption.

Encryption can be used between data processing machines and data storage devices such as magnetic tape and magnetic disk. In this application, the data is encrypted before it is written on the storage device and decrypted before it is subsequently read. Data is stored in its cipher form and transformed to plaintext only when it is to be processed within the computer.

Encryption can be used to authenticate the identities of users, terminals, and computers of a data processing system. Passwords have historically been used to differentiate between friend and foe during times of war. Knowledge of the secret password was accepted as authenticating the identity of friends. Unique identification was not necessary and the password was changed for each mission. The DES uses a key, similar to a password, which must be supplied to each group of users of the algorithm. Having the correct key authenticates an individual to a data processing system.

In a similar manner a terminal or a computer may be authenticated as an authorized device of a data processing system. Supplying the correct key to a DES device when requested by the authorization system can authenticate a terminal associated with the device. This authorization system may be a special program or a special computer system which has been established to control access to the resources and data of the overall system. The authorization system must be initialized with the identities and the authentication keys of all authorized users and devices of the system. This system will issue a challenge for proper identification whenever a device or individual wishes to access the system. Similar challenge.response password systems are currently in use for computer user authentication. When combined with data encryption technology, authorization systems can authenticate the claimed identities of users and devices without compromising the passwords or keys by transmitting them through the system.

2.4 When Should Data Encryption Be Used?

Data encryption should be used whenever it is the most cost effective method available to protect the confidentiality or integrity of the data. Confidentiality refers to the accidental or intentional disclosure of data to an unauthorized individual. Integrity refers to data which has not been exposed to accidental or malicious alteration or destruction. Encryption of data prevents unauthorized recipients of the cipher from interpreting its meaning. Encryption can also prevent unauthorized individuals from manipulating the cipher in such a way that the original data is changed in a predetermined manner. To be effective, encryption must cost less than the expected loss (risk) if the protection were not provided. Computation or estimation of costs and risks and the decision to employ cryptographic protection are management functions of the authority responsible for the data. Risk analysis information may be found in FIPS PUB 65 [6].

2.5 Why Is a Data Encryption Standard Necessary?

A data encryption standard is needed to protect sensitive or valuable data within Federal computer systems and networks. Effective sharing of computational facilities and controlled sharing of computer data have been retarded pending development of adequate protection measures. Data encryption techniques are needed for controlling access to sensitive data in multiuser computer systems, for protecting the integrity of transactions in national and international monetary transfer systems, for disguising sensitive data during transmission, and for authenticating the users and devices of distributed computer systems and networks. A myriad of different encryption algorithms would result in a fundamental incompatibility of data communications equipment. Research and development in cryptographic algorithms are difficult areas; redundant and unusable results often occur. Support of several standards would incur a higher cost for the Federal Government. The Data Encryption Standard provides a basic method for more effective computer utilization and a high level of protection for computer data.

The need to interface with the data processing facilities of Federal agencies may make it desirable that private organizations have and be able to use the DES. Since its adoption as a Federal Standard, the DES algorithm has been approved as a standard by the American National Standards Institute [1] and recommended for use by the American Bankers Association [7].

2.6 What Are the Requirements of a DES?

An encryption algorithm must satisfy the following requirements in order to be acceptable as a Federal standard:

1. It must provide a high level of security.
2. It must be completely specified and easy to understand.
3. The security provided by the algorithm must not be based upon the secrecy of the algorithm.
4. It must be available to all users and suppliers.
5. It must be adaptable for use in diverse applications.
6. It must be economical to implement in electronic devices and be efficient to use.
7. It must be amenable to validation.

8. It must be exportable.

The algorithm described in FIPS PUB 46 satisfies all these requirements.

2.7 What Role Has NBS Played in the DES?

NBS has the responsibility for developing Federal Information Processing Standards through Public Law 89.306 and Executive Order 11717. The Institute for Computer Sciences and Technology (ICST) has the responsibility within the NBS to recommend and coordinate standards and guidelines for improved computer utilization and information processing within the Federal Government, as well as for developing the technology needed to support these standards activities. Because of the unavailability of general cryptographic technology outside the national security arena, and because security provisions, including encryption, were needed in unclassified applications involving Federal Government computer systems, NBS initiated a computer security program in 1973 which included the development of a standard for computer data encryption. Since Federal standards impact on the private sector, NBS solicited the interest and cooperation of industry and user communities in this work.

In May 1973, NBS published a notice in the Federal Register (38FR12763) inviting the submission of data encryption algorithms and techniques which might be considered for use in a

Federal standard. The responses showed considerable interest in and need for such protection. A second Federal Register solicitation (39FR30961) in August 1974 reiterated the former solicitation and provided a further opportunity to submit data encryption algorithms. Subsequent to the closing of the solicitation, algorithms submitted to NBS were evaluated for technical feasibility as a Federal standard. This document discusses the algorithm which satisfied the requirements of a data encryption standard. It was developed by the International Business Machines Corporation (IBM). IBM made the specifications of the algorithm available to NBS for publication as a Federal Information Processing Standard (FIPS) and has provided nondiscriminatory and royalty free licensing procedures for building electronic devices which implement the algorithm. At the request of NBS, the National Security Agency (NSA) conducted an exhaustive technical analysis of the DES. No shortcuts or secret solutions were found and, as a result, NSA confirmed the soundness of the DES's encryption principle and its suitability to protect unclassified Federal data [8]. NBS published the algorithm in the Federal Register in March 1975 (40FR12067) for public comment and published the proposed standard in the Federal Register in August 1975 (40FR32395) for public comment. In January 1977 the algorithm was published as a Federal standard, FIPS PUB 46 [2].

3. DATA ENCRYPTION METHODS

3.1 Basic Methods

Encryption is a transformation of data from its original, intelligible form to an unintelligible cipher form. Two basic transformations may be used: permutation and substitution. Permutation changes the order of the individual symbols comprising the data. In a substitution transformation, the symbols themselves are replaced by other symbols. During permutation the symbols retain their

2.6 What Are the Requirements of a DES?

An encryption algorithm must satisfy the following requirements in order to be acceptable as a Federal standard:

1. It must provide a high level of security.
2. It must be completely specified and easy to understand.
3. The security provided by the algorithm must not be based upon the secrecy of the algorithm.
4. It must be available to all users and suppliers.
5. It must be adaptable for use in diverse applications.
6. It must be economical to implement in electronic devices and be efficient to use.
7. It must be amenable to validation.
8. It must be exportable.

The algorithm described in FIPS PUB 46 satisfies all these requirements.

2.7 What Role Has NBS Played in the DES?

NBS has the responsibility for developing Federal Information Processing Standards through Public Law 89.306 and Executive Order

11717. The Institute for Computer Sciences and Technology (ICST) has the responsibility within the NBS to recommend and coordinate standards and guidelines for improved computer utilization and information processing within the Federal Government, as well as for developing the technology needed to support these standards activities. Because of the unavailability of general cryptographic technology outside the national security arena, and because security provisions, including encryption, were needed in unclassified applications involving Federal Government computer systems, NBS initiated a computer security program in 1973 which included the development of a standard for computer data encryption. Since Federal standards impact on the private sector, NBS solicited the interest and cooperation of industry and user communities in this work.

In May 1973, NBS published a notice in the Federal Register (38FR12763) inviting the submission of data encryption algorithms and techniques which might be considered for use in a Federal standard. The responses showed considerable interest in and need for such protection. A second Federal Register solicitation (39FR30961) in August 1974 reiterated the former solicitation and provided a further opportunity to submit data encryption algorithms. Subsequent to the closing of the solicitation, algorithms submitted to NBS were evaluated for technical feasibility as a Federal standard. This document discusses the algorithm which satisfied the requirements of a data encryption standard. It was developed by the International Business Machines Corporation (IBM). IBM made the specifications of the algorithm available to NBS for publication as a Federal Information Processing Standard (FIPS) and has provided nondiscriminatory and royalty free licensing procedures for building electronic devices which implement the algorithm. At the request of NBS, the National Security Agency (NSA) conducted an exhaustive technical analysis of the DES. No shortcuts or secret solutions were found and, as a result, NSA confirmed the soundness of the DES's encryption principle and its suitability to protect unclassified Federal data [8]. NBS published the algorithm in the Federal Register in March 1975 (40FR12067) for public comment and published the proposed standard in the Federal Register in August 1975 (40FR32395) for public comment. In January 1977 the algorithm was published as a Federal standard, FIPS PUB 46 [2].

3. DATA ENCRYPTION METHODS

3.1 Basic Methods

Encryption is a transformation of data from its original, intelligible form to an unintelligible cipher form. Two basic transformations may be used: permutation and substitution. Permutation changes the order of the individual symbols comprising the data. In a substitution transformation. the symbols themselves are replaced by other symbols. During permutation the symbols retain their

3.5 Recirculating Block Product Cipher

A block product cipher may be constructed by using a permutation operation and a substitution operation alternately and recirculating the output of one pair of operations back into the input for some number of iterations. Each iteration is called a round. A cipher produced in this way is termed a recirculating block product cipher. If a recirculating block product cipher is properly constructed with an unknown key, then the alteration of a single bit of the plaintext block will unpredictably alter each bit of the ciphertext block. Altering a bit of the ciphertext. will also result in an unpredictable change to the plaintext block after decryption.

3.6 Characteristics of the DES Algorithm

The DES algorithm is a recirculating, 64-bit, block product cipher whose security is based on a secret key. DES keys are 64-bit binary vectors consisting of 56 independent information bits and eight parity bits. The parity bits are reserved for error detection purposes and are not used by the encryption algorithm. The 56 information bits are used by the enciphering and deciphering operations and are referred to as the active key. Active keys are generated (selected at random from all possible keys) by each group of authorized users of a particular computer system or set of data. Each user should understand that the key must be protected and that any compromise of the key will compromise all data and resources protected by that key.

In the encryption computation the 64-bit data input is divided into two halves each consisting of 32 bits. One half is used as input to a complex nonlinear function, and the result is exclusive OR'ed to the other half. (See fig. 5.1.) After one iteration, or round, the two halves of the data are swapped and the operation is performed again. The DES algorithm uses 16 rounds to produce a recirculating block product cipher. The cipher produced by the algorithm displays no correlation to the input. Every bit of the output depends on every bit of the input and on every bit of the active key.

The security provided by the DES algorithm is based on the fact that, if the key is unknown, an unauthorized recipient of encrypted data, knowing some of the matching input data, must perform an unacceptable effort to decipher other encrypted data or recover the key. Even having all but one bit of the key correct does not result in intelligible data-

The only known way of obtaining the key with certainty is by obtaining matched ciphertext and plaintext and then by exhaustively testing keys by enciphering the known plaintext with each key and comparing the result with the known ciphertext. Since 56 independent bits are used in a DES key, 2_{56} such tests are required to guarantee finding a particular key. The expected number of tests to recover the correct key is 2_{55}. At one microsecond per test 1142 years would be required. Under certain conditions (not only knowing matched plaintext and ciphertext but also the complement of the plaintext and the resulting ciphertext) the expected effort would be reduced to 571 years. The possibility of 2_{56} keys (approximately 70 quadrillion) makes the guessing or computing of any particular key very unlikely given that the guidelines for generating and protecting a key provided in this publication are followed. Of course, one can always reduce the time required to exhaust any cryptoalgorithm by having several devices working in parallel. Time is reduced but initial expenses are increased.

An important characteristic of the DES algorithm is its flexibility for usage in various data processing applications. Each cipher block is independent of all others allowing encryption or decryption of a single block in a message or data structure. Random access to encrypted data is therefore possible. The algorithm may be used in this straightforward way to form a block cipher or alternatively used with chaining in which the output of the algorithm depends on previous results of the algorithm. The first technique is called the Electronic Codebook (ECB) mode and the chaining technique has two examples (discussed in these guidelines) called the Cipher Block Chaining (CBC), mode and the Cipher Feedback (CFB) mode. In addition, DES may be used in the Output Feedback (OFB) mode to generate a pseudorandom stream of bits which is exclusive OR'ed to the plaintext bits to form cipher. These will be discussed in 5.3.

The DES algorithm is mathematically a one.to-one mapping of the 264 possible input blocks onto all 264 possible output blocks. Since there are 256~ possible active keys, there are 264 ~ possible mapping Selecting one key selects one of the mapping.

The input to the algorithm is under complete specification of the designer of the cryptographic system and the user of the system. Any pattern of 64 bits is acceptable to the algorithm. The format of a data block may be defined for each application. In the ECB mode, the subfields of each block may be defined to include one or more of the following: a block sequence number, the block sequence number of the last block received from the transmitter, error detecting/correcting codes, control information, date and time information, user or terminal authentication information, or a field in which random data is placed to ensure that identical data fields in different input blocks will result in different cipher blocks. It is recommended that no more than 16 bits be used for known constant values. For example, the same 32-bit terminal identification value should not be used in every block. If it is desired that data blocks in the ECB mode display a sequence dependency, a portion of the last sent or last received block may be incorporated into the block, either as a subfield or exclusive OR'ed to the block itself.

The DES algorithm is composed of two parts: the enciphering (encryption) operation and the deciphering (decryption) operation. The algorithms are functionally identical except that the selected portion of the key used for rounds 1,2 16 during the encryption operation are used in the order 16,15 1 for the decryption operation. The algorithm uses two 28-bit registers called C and D to hold the 56-bit active key. The key schedule of the algorithm circularly shifts the C and D registers independently, left for encryption and right for decryption. (See fig. 5.3 and table 5.4.) If the bits of the C register are all zeros or all ones (after Permuted Choice 1 is applied to the key) and the bits of the D register are all zeros or all ones, then decryption is identical to encryption. This occurs for four known keys: (O1O1O1O1O1O1O1O1), (FEFEFEFEFEFEFEFE), (1F1F1F1FOEOEOEOE), and (EOEOEOEOF1F1F1F1). [Note that the parity bits of the key are set so that each 8-bit byte has odd parity.] It is likely that, in all other cases, data encrypted twice with the same key will not result in plaintext (the original, intelligible data form). This characteristic is beneficial in some data processing applications in that several levels of encipherment can be utilized in a computer network even though some of the keys used could be the same. If an algorithm is its own inverse, then an even number of encryptions under the same key will result in plaintext.

There are certain keys such that for each key K there exists a key K' for which encryption with K is identical to decryption with K' and vise versa. K and K' are called dual keys. Keys with duals were found by examining the equations which must hold in order for two keys to have reversed key schedules. Keys having duals are keys which produce all zeros, all ones, or alternating zero-one patterns in the C and D registers after Permuted Choice 1 has operated on the key. (See fig. 5.3.) These keys are listed below.

	KEY	DUAL
1.	EOO1EOO1F1O1F1O1	O1EOO1EOO1F1O1F1
2.	FE1FFE1FFEOEFEOE	1FFE1FFEOEFEOEFE
3.	EO1FEO1FFIOEFIOE	1FEO1FEOOEF1OEF1
4.	O1FEO1FEO1FEO1FE	FEO1FEO1FEO1FEO1
5.	O11FO11FO1OEO1OE	1FO11FO1OEO1OEO1
6.	EOFEEOFEF1FEF1FE	FEEOFEEOFEF1FEF1
7.	O1O1O1O1O1O1O1O1	O1O1O1O1O1O1O1O1
8.	FEFEFEFEFEFEFEFE	FEFE1EFEFEFEFEFE
9.	EOEOEOEOF1F1FIF1	EOEOEOEOF1F1F1F1
10.	1F1F1F1FOEOEOEOE	1F1F1F1FOEOEOEOE

The first 6 keys have duals different than themselves, hence each is both a key and a dual giving 12 keys with duals. The last four keys equal their duals, and are called self-dual keys. These are the four previously discussed keys for which double encryption equals no encryption, i.e., the identity mapping. The dual of a key (which has a dual) is formed by dividing the key into two halves of eight hexidecimal characters each and circular shifting each half by two characters. No other keys are known to exist which have duals.

Data may be decrypted first and then encrypted (rather than encrypted and then decrypted) and result in plaintext. Plaintext may be encrypted several times and then decrypted the same number of times with the same key and result in plaintext. Similarly, data may be encrypted successively by

different keys and decrypted sucessively by the same keys to produce the original data, if the decryption operations are performed in the proper (inverse) order. If $D_1(E_1(P)) = P$ is read "Encrypting plaintext with Key 1 and then decrypting the result with Key 1 yields the plaintext," then the following are true:

1. $E_1(D_1P)) = P$

2. $E_1(E_1(P)) = P$ for self-dual keys
3. $D_1(D_1(E_1(E_1(P)))) = P$
4. $E_1(E_1(D_1(D_1(P)))) = P$
5. $D_1(D_2(E_2(E_1(P)))) = P$
6. $D_1(D_2(...(D_j(E_j..(E_2(E_1(P)...) =P$
7. $E_1(E_2(...(E_j(D_j...(D_2(D_1(P)...)=P$
8. $E_2(E_1(P)) = P$ for dual keys
9. $D_2(D_1(P)) = P$ for dual keys

but in general the following is not true:

10. $D_2D_1(E._2(E_1(P)))) =$

4. SECURITY THREATS REDUCED THROUGH ENCRYPTION

Encryption may be implemented in a computer system in order to combat several possible threats to the security of computer data. These threats are generally categorized as transmission threats and storage threats. Security against these threats is generally termed communication security (COMSEC) or file security (FILESEC). The DES algorithm can be used in both applications but the key will be handled differently. The generation, distribution, protection, and destruction of cryptographic keys are generically referred to as key management and are discussed in section 6.

4.1 Transmission Threats

Encryption can be used to prevent the disclosure of data and to detect the modification of transmitted data. Encryption will not combat the threats of accidental or deliberate destruction. Encrypted data can be lost or destroyed as easily as unencrypted data◦ Adequate backup facilities or copies must be provided to recover from the destruction of either encrypted or unencrypted dab In addition, destruction or loss of the key used to encrypt data is equivalent to the loss or destruction of the data itself.

The following is a list of threats that are countered with the encryption of transmitted data:

l. Spoofing: Spoofing is the threat of accepting a false claim of identity. Spoofing by a computer system penetrator is a serious threat at many places in a computer system. The computer's data communication system is especially vulnerable to spoofing. The identities of terminals, computers, and users can often be simulated so that the receiving device cannot discern a true identity from a falsely claimed identity. Data encryption can be used for authentication by requiring that a unique encryption key be associated with each identity. Successful communication using this key mutually authenticates the holders of the key (provided that the key has not been compromised) and thus prevents spoofing. If the key is not known, false messages cannot be correctly generated and entered into the system and hence message spoofing is prevented.

2. Misrouting: The threat of misrouting is directly proportional to the complexity of the communication system and inversely proportional to the reliability of its components. A simple message routing indicator scheme combined with encryption of the routing indicator may be used to detect misrouting, but prevention can only be accomplished with dedicated lines and permanent connections. In any but

geographically local systems, the prevention of misrouting is not economically feasible. However, data encryption can prevent the unauthorized use of misrouted data.

3. Passive Wiretapping (Monitoring): Monitoring of messages during data transmission can occur all along the transmission path in any of several ways. Wiretapping or radio reception of the transmitted data are the most common methods. The transmission is not delayed or altered, only monitored or copied. This threat is difficult to combat in any way other than physically protecting the transmission path or encrypting the data. Plaintext is also vulnerable to monitoring due to radiation, conduction, and acoustic pickup during input and output operations. These threats are prevalent in high voltage CRT terminals, electrically connected devices, and mechanical printing or punching devices. Encryption protects the plaintext from disclosure. The encryption devices should be designed to be an integral part of the original source equipment and the final destination equipment whenever possible. The data encryption devices themselves must be physically protected and designed to minimize electronic emanations.

4. Active Wiretapping: With this type of communication threat the communication line is broken, a high speed receiver-transmitter is installed, and the intercepted data is retransmitted unchanged until a special "looked for" event causes the tapping mechanism to modify the data so as to have false information accepted as valid. Communications will be slightly delayed while the data is being modified but this delay is often not detectable because other variable length delays are already in the communication system. Encryption prevents the penetrator from intelligently modifying the cipher so that the decrypted plaintext is ungarbled (i.e., readable and acceptable). Special precautions must be utilized to prevent either the playback threat or the substitution threat. The former consists simply of copying a valid encrypted message and playing it back (retransmitting it) to the unsuspecting receiver. If the key has not been changed, the receiver will correctly decrypt the message and may accept it. For certain types of messages (funds deposits, merchandise orders, etc.), this could have disastrous results. The substitution threat consists of replacing blocks or characters of 1= ciphertext with other blocks or characters without actually deciphering the data or having the key.
The perpetrator substitutes the cipher of known plaintext. This can be accomplished in the block mode if each block is totally independent

from all others, and no other block or message authentication system is used.

4.2 Storage Threats

In addition to combatting threats to computer data security during transmission among terminals and computers, the DES may be used effectively for protecting computer data during storage, but the system implementation will be different in the two cases. In the transmission case, the cryptographic key must be available at the two participating locations simultaneously and may be destroyed when that transmission is complete. In the storage case, the key need be at only one location but must be retained for reuse when the data is to be retrieved and used. The computer system or the user must be able to provide the key at the appropriate place and at the appropriate time.

The following is a list of threats that are countered with the encryption of stored data:

1. Theft: Encryption of stored computer data provides protection against the disclosure of stolen data. Data may be stolen from on-line devices (disks, mass storage devices, etc.) by unauthorized access, or from off-line devices (magnetic tape, cards, disk packs, etc.) by physically removing the device and reading it on another computer system. In addition if there is a threat of a computer data storage facility or a computer center being taken over by force, bulk encryption of all data using a common key which is easily erased from the encryption device effectively renders the data unreadable and unusable by destroying the key. This key must be kept in a physically secure location (safe, etc.) so that it may be reentered into the encryption device when the facility has been made secure again. User controlled encryption of private data files renders the data unreadable to other system users.

2. Residue: Data that is left on magnetic media and not erased after it is no longer needed is called residue. Erasing computer data on magnetic storage media may be a very time consuming process. Overwriting data which is to be discarded in a shared system can use a significant amount of input and output time if done as standard practice. Data recovered by simply reading discarded data that was not destroyed is considered to be "scavenged." If sensitive data is always stored on the media in an encrypted form, tapes and disk packs may be returned to their supplier when no longer

needed or the "scratched" data tapes may be reused without erasing. Merely destroying the key precludes use of the data. System failures during the erasing of magnetic media are no longer a concern if the media are encrypted. Encryption of stored data with the user's private key obviates the need for clearing temporary storage after use.

3. Remanence: Remanence is the magnetic flux remaining in a magnetic substance after the magnetic force has been removed. In some magnetic storage media, data stored for a long period of time on the media can remain at a lower signal intensity level even after the media have been erased. Encryption of all sensitive data stored on such media removes this threat and such storage media may be released for general usage rather than destroyed. It should be noted that for unclassified computer data, this is a very insignificant threat and encryption should not be justified for this reason alone.

4. Addressing Failure: Random access magnetic storage media have a physical addressing mechanism which positions the data under the reading heads and transfers the data. Software data access methods generally have a complex data structure associated with the stored data to optimize access to it. Both of these mechanisms have a small, but non zero, probability of failure. Encrypting the data by combining the location of the data with the key can prevent accidental reading of the wrong data. Applications of this type in the system will depend greatly on the implementation of the DES device in the proper place in the system architecture.

5. IMPLEMENTATION OF THE ALGORITHM

A cryptographic system comprises many components, e.g., a cryptographic algorithm, a key management system, an applications interface, a maintenance procedure, and a user training program. Section 5 discusses the basic implementation of the DES algorithm in electronic devices and methods of interfacing it to particular applications.

A hardware implementation of the DES algorithm is described and a software interface is outlined. The device performs the mathematical transformation described in the DES. The software interface provides control functions to the device, receives status information from the device, and implements the Cipher Block Chaining (CBC), Cipher Feedback (CFB), or Output Feedback (OFB) modes of operation discussed in 5.3. This approach provides a flexible mechanism for use in many data processing environments, but it may not provide adequate efficiency or security in all cases. For example, special hardware may be required for very high speed or error sensitive applications.

5.1 Basic Implementation

Basic implementation refers to the embodiment of the DES algorithm. FIPS PUB 46 specifies that electronic hardware is required for the basic implementation.

5.1.1 Electronic Devices

The NBS DES algorithm specifies the encryption of 64 bits of data into a 64-bit cipher based on a 56-bit active key, and the decryption of a 64-bit cipher block into a 64-bit data block based on a 56-bit active key. The steps and the tables of the algorithm are completely specified and no options to the basic algorithm are contained in the DES. However, there are many ways to incorporate the algorithm into a cryptographic system and the implementation used will depend on the application. A recommended method is to implement the basic DES algorithm in a special purpose electronic
V device and then control it from a programmable computer (e.g., a microprocessor). Some of the issues involved in the application of the DES are: how is the input formatted, is the data itself or a different 64-bit value used as input to the algorithm, how is the key generated and distributed, and how often is the key changed?

Implementation of the DES algorithm in special purpose electronic devices provides the following economic and security benefits:

1. Efficiency of algorithm operation is much higher in specialized electronic devices.
2. Basic implementation of the algorithm in specialized LSI electronic devices which can be used in many applications and environments should result in cost savings to the user through high volume production.
3. Functional operation of the device may be tested and validated independently of the environment in which it is used.
4. An encryption key may be entered directly into the device without appearing elsewhere in the computer system.
5. Unauthorized modification of the algorithm is very difficult in such a device.
6. Independent devices may encipher the data simultaneously and the output may be tested before the cipher is transmitted.
7. The control and data paths, to and from the device, may be controlled and monitored.

For these reasons, implementation in special purpose devices (electronic devices or read only memories) is required by FIPS PUB 46.

5.1.2 Basic Implementation Control Functions

Several control functions must be available in the basic implementation of the algorithm. The actual controls that are provided in an electronic implementation will vary according to the technology used and the packaging available. The following discussion presents a set of controls designed and implemented by the NBS technical staff in two identical hardware devices being used in the NBS Data Encryption Testbed. The two DES test units were designed and built in medium scale integration (MSI) TTL logic. The Data Encryption Testbed based on these units is described in
5-5.

Control lines are used to provide control signals to the DES device; status lines are used to monitor the condition of the DES device; data lines are used to input and output the plain and enciphered data. In the NBS implementation, eight data input lines and eight data output lines are used. Both the data and key needed by the algorithm are entered via the data lines in 8-bit bytes. Similarly, when the encryption or decryption operation is complete, the plaintext or ciphertext is sequentially read from the device in 8-bit bytes.

CONTROL LINES

1. Data/Key-Enter data (0) or enter key (1).

2. Encipher/Decipher-Encipher data (0) or decipher data (1).

3. Plain/Cipher-Enter plain key (0) or enter enciphered key (1).

4. Reset except key (1)-Clears all internal registers except key register.

5. Reset (1)-Clears all internal registers.

6. Input ready (1)-Input lines are ready to be read into the DES device.

7. Output accepted (1)-Output lines have been read by the controlling device.

STATUS LINES

1. Busy (1)-Device is busy and cannot input or output.

2. Parity error (1)-Key being entered has a parity error.

3. Control error (1)-The control last given to the DES is incorrect.

4. Output ready (1)-Output lines are ready to be read.

5. Input accepted (1)-Input lines have been read.

The NBS implementation is designed for use as an encryption testbed device and for use as a DES validation device. The testbed has been designed to develop control procedures for DES devices in various applications and for different communications protocols. For demonstration purposes, digital displays of data, control and status are provided on the front panel of the device.

Two units have been constructed to provide a test facility for data communications. The NBS DES device is capable of either enciphering or deciphering a block of data in nine microseconds, once the data has been loaded. In addition, it takes a minimum of twenty microseconds to either load or unload the device.

A separate unit was built to operate the DES device manually. This unit has two sets of 16 rotary thumbwheel switches: 16 for the data and 16 for the key. Each switch has 16 positions: hexadecimal digits 0-9 and A.F. These allow 64-bit entry of key, plaintext, and cipher into the DES device. The test unit also contains control buttons and binary switches to provide the control signals necessary for operating the DES. The test unit is only used for off-line demonstrations of the DES devices and for maintenance testing.

5.2 Secondary Implementation

The secondary implementation consists of the control mechanisms which govern the operation of the basic implementation. It is also responsible for implementing the CBC, CFB, and OFB modes of operation which are discussed in section 5.3. Each NBS DES device is connected to a microprocessor computer with a multiline cable as a parallel interface. This interface contains the data input and output lines, the control lines, and the status lines. The DES device input lines and the control lines are connected to output ports of the microprocessor. The DES device output lines and the status lines are connected to input ports of the microprocessor. The DES device looks like a simple input-output device to the microprocessor.

5.2.1 Secondary Implementation Control Functions

A DES device must be contained in a control environment that conforms to the requirements of a particular application. This environment includes electrical power, control and status lines, data lines for input and output, and the capability of providing other special services that will depend on the application. One such service is to collect and enter the data into the DES primary device in accordance with the data format and communication protocol specifications. Another service is to receive the output from the DES device and then present it to the communication system.

In any encrypted communications application other than link encryption (i.e., cryptographic protection of a communication line or path having no intermediary nodes), addressing and related control information must be available in an unencrypted form. Separating sensitive information from control information is a very crucial security task of the secondary device.

5.2.2 Error Handling

Errors associated with the primary encryption device should be detected and handled by the secondary device. Physical tampering detectors (vibration or intrusion sensors) may be used to detect physical tampering or unauthorized access to the encryption unit. Sensors which detect abnormal changes in the electrical power or the temperature may be used to monitor physical environment changes which could cause a security problem. However, the major requirement for error detection or correction involves the application itself. The type of error control utilized will depend on the sensitivity of the data and the application. The method selected may range from no error handling capability for some systems to full redundancy of encryption devices in other systems. Errors may be ignored when detected or the entire system may be immediately shutdown. Errors which could compromise the plaintext or key should never be ignored.

5.3 Modes of Operation

The DES algorithm specifies a mathematical transformation of a 64-bit input block to a 64-bit output block using a key. Specific examples of this transformation are given in NBS Special Publication 500-20 [5]. $E_K(I) = O$ and $D_K(O) = I$ are read "Enciphering the input I using key K